

9

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-096121

(43)Date of publication of application : 09.04.1999

(51)Int.Cl.

G06F 15/00

(21)Application number : 09-253960

(71)Applicant : KOKUSAI ELECTRIC CO LTD

(22)Date of filing : 18.09.1997

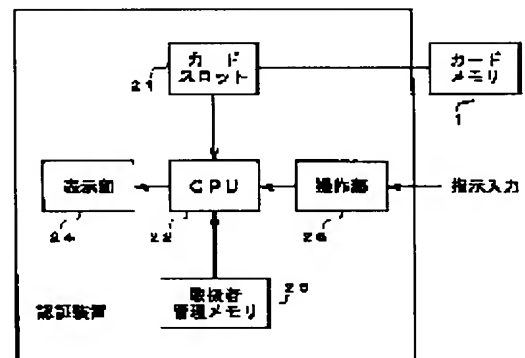
(72)Inventor : KAYANUMA TAKAAKI  
TAKAZAWA HIDEAKI  
TAKECHI EIJI

### (54) CERTIFICATION DEVICE AND CERTIFICATION SYSTEM

#### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a certification device and a certification system capable of preventing a card memory from being illegally used even when it is copied.

**SOLUTION:** When a CPU 22 attains certification, the certification device changes a certification code stored in a card memory 1 inserted into a card slot 21 and a handler management memory 23 and completing its certification. When the CPU 22 attains certification, the device changes a certification code stored in the card memory 1 inserted into the card slot 21 and a handler management memory 33 on a server and completing its certification.



(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平11-96121

(43)公開日 平成11年(1999)4月9日

(51)Int.Cl.<sup>8</sup>

G 0 6 F 15/00

識別記号

3 3 0

F I

G 0 6 F 15/00

3 3 0 G

審査請求 未請求 請求項の数7 O L (全 8 頁)

(21)出願番号 特願平9-253960

(22)出願日 平成9年(1997)9月18日

(71)出願人 000001122

国際電気株式会社

東京都中野区東中野三丁目14番20号

(72)発明者 董 昭 陸 昭

東京都中野区東中野三丁目14番20号 国際  
電気株式会社内

(72)発明者 高 沢 秀 明

東京都中野区東中野三丁目14番20号 国際  
電気株式会社内

(72)発明者 武 地 永 次

東京都中野区東中野三丁目14番20号 国際  
電気株式会社内

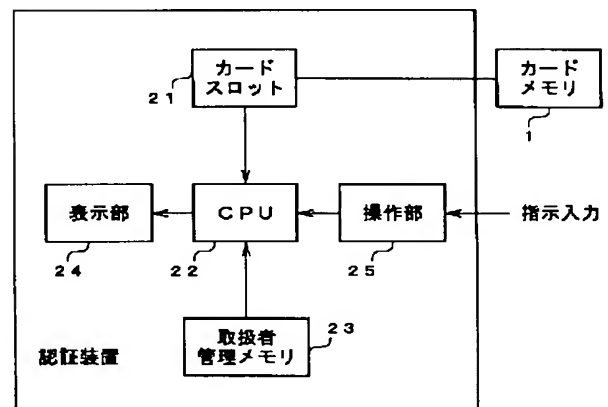
(74)代理人 弁理士 船 津 暢 宏 (外 1 名)

(54)【発明の名称】 認証装置及び認証システム

(57)【要約】

【課題】 従来の認証装置及び認証システムでは、カードメモリがコピーされると不正使用される虞があったが、本発明では、カードメモリがコピーされても不正使用を防止できる認証装置及び認証システムを提供する。

【解決手段】 CPU 22が認証を達成したときに、カードスロット 21に挿入されているカードメモリ 1と取扱者管理メモリ 23とに格納されている、認証が為された認証コードを変更する認証装置及び、CPU 22が認証を達成したときに、カードスロット 21に挿入されているカードメモリ 1とサーバ 3上の取扱者管理メモリ 33とに格納されている、認証が為された認証コードを変更する認証システムである。



**【特許請求の範囲】**

【請求項 1】 認証が為される毎に認証コードを変更することを特徴とする認証装置。

【請求項 2】 メモリカードのインターフェイスであるカードスロットと、認証コードを格納する取扱者管理メモリとを具備し、認証が為されると、前記取扱者管理メモリに格納されている認証が為された認証コードを特定のコードで上書きして変更し、前記カードスロットに挿入されたメモリカードの認証コードを前記特定のコードで上書きして変更することを特徴とする認証装置。

【請求項 3】 メモリカードのインターフェイスであるカードスロットを具備する認証装置と、認証コードを格納する取扱者管理メモリを具備するサーバとを備え、前記認証装置で認証が為されると、前記認証装置が特定のコードとともに前記サーバに前記取扱者管理メモリに格納されている認証が為された認証コードを当該特定のコードで上書きして変更する要求を送信出力し、前記カードスロットに挿入されたメモリカードの認証コードを前記特定のコードで上書きして変更し、前記サーバが、受信した前記要求にしたがって、前記取扱者管理メモリに格納されている前記認証コードを前記特定のコードで上書きして変更することを特徴とする認証システム。

【請求項 4】 認証が為されないと、当該認証が為されなかったユーザ名による装置の使用を以後できないようにすることを特徴とする請求項 2 記載の認証装置。

【請求項 5】 認証が為されないと、当該認証が為されなかったユーザ名による装置の使用を以後できないようにすることを特徴とする請求項 3 記載の認証システム。

【請求項 6】 特定のコードは、認証が為された時刻を表すコードであることを特徴とする請求項 2 又は請求項 4 記載の認証装置。

【請求項 7】 特定のコードは、認証装置において認証が為された時刻を表すコードであることを特徴とする請求項 3 又は請求項 5 記載の認証システム。

**【発明の詳細な説明】****【0001】**

【発明の属する技術分野】本発明は、ICカード等のカードメモリを利用して装置取扱者の認証を行う認証装置及び認証システムに係り、特に不正使用の防止をより強化できる認証装置及び認証システムに関する。

**【0002】**

【従来の技術】認証装置は、不正使用を防止しようとする装置に装着し、利用者の認証が為されるまでは、当該装置の操作を禁止する動作を行うものである。

【0003】一般的な認証装置及び認証システムについて、図 1 と図 2 とを参照しつつ説明する。図 1 は、認証装置の一般的な構成ブロック図であり、図 2 は、認証システムの一般的な構成ブロック図である。

【0004】図 1 に示す認証装置は、カードメモリ 1 を

挿入され、当該カードメモリ 1 のインターフェイスとして動作するカードスロット 2 1 と、CPU 2 2 と、取扱者管理メモリ 2 3 と、表示部 2 4 と、操作部 2 5 とから構成されている。

【0005】また、図 2 に示す認証システムは、カードスロット 2 1 と、CPU 2 2 と、表示部 2 4 と、操作部 2 5 と、送受信部 2 6 と、サーバ 3 とから構成されている。さらに、サーバ 3 は、送受信部 3 1 と、CPU 3 2 と、取扱者管理メモリ 3 3 とから構成されている。尚、図 2 に示す認証システムでは、複数の認証装置がネットワーク等を介してサーバ 3 に接続されていても構わない。

【0006】まず、図 1 に示す認証装置について、以下、各部を具体的に説明する。カードメモリ 1 は、ユーザ名と認証コードとを対応づけて格納しているものであり、具体的には、図 4 に示すような内容のテーブルを格納しているものである。図 4 は、カードメモリ 1 に格納されているテーブルの内容の一例を表す説明図である。

【0007】CPU 2 2 は、操作部 2 5 から装置を使用しようとする旨の指示の入力を受けて、取扱者管理メモリ 2 3 と、カードスロット 2 1 に差し込まれたカードメモリ 1 の内容と、操作部 2 5 から入力される操作の内容とを参照して規定の条件が満たされれば、装置の使用を許可するものである。CPU 2 2 における具体的な処理は後述する。

【0008】取扱者管理メモリ 2 3 は、図 5 に示すような内容のテーブルを格納しているものである。図 5 は、取扱者管理メモリ 2 3 の内容の一例を表す説明図である。

【0009】ここで、CPU 2 2 における認証の処理について図 6 を参照しつつ説明する。図 6 は、CPU 2 2 における認証の処理を表すフローチャート図である。CPU 2 2 は、操作部 2 5 から装置を使用しようとする旨の指示の入力を受けて、カードスロット 2 1 にカードメモリ 1 が挿入されているか否かを調べる（S 1）。

【0010】そして、カードメモリ 1 が挿入されていない（N o ならば）、表示部 2 4 にカードが挿入されていない旨のメッセージを表示出力し（S 2）、処理終了する。

【0011】また、処理 S 1 において、カードスロット 2 1 にカードメモリ 1 が挿入されていれば（Y e s であれば）、該カードメモリ 1 からユーザ名と認証コードとを読み出し（S 3）、取扱者管理メモリ 2 3 から対応するユーザ名を検索し、それに対応するパスワードを読み出す（S 4）。

【0012】そして、CPU 2 2 は、パスワードを要求する旨のメッセージを表示部 2 4 に表示出力し（S 5）、利用者から操作部 2 5 を介してパスワードの入力を受けて、それが処理 S 4 にて取扱者管理メモリ 2 3 から読み出したパスワードと一致するか否かを調べる（S

6)。

【0013】ここで、パスワードが一致しないと（Noであると）、パスワードが異なる旨のメッセージを表示部24に表示出力し（S7）、処理終了する。また、処理S6において、パスワードが一致すると（Yesであると）、取扱者管理メモリ23から処理S4と同様に先に検索されるユーザ名に対応する認証コードを読み出す（S8）。

【0014】そして、CPU22は、処理S3にてカードメモリ1から読み出した認証コードと取扱者管理メモリ23から読み出した認証コードとが一致するか否かを調べ（S9）、一致すれば（Yesならば）、認証が達成され、装置の操作を許可し（S10）、処理終了する。

【0015】また、処理S9において、認証コードが一致しなければ（Noならば）、表示部24に「カードメモリが違います」等のメッセージを表示出力して（S11）、処理を終了する。

【0016】次に、図1に示す認証装置の動作について説明する。尚、以下の説明では、取扱者管理メモリ23には、図5に示すようなテーブルが格納されているものとする。すなわち、ユーザ名「TKAYA」には、パスワードとして「1」と、認証コードとして「TK1」とが対応づけられているとする。

【0017】装置の利用者は、認証装置のカードメモリ1をカードスロット21に挿入し、CPU22に装置を使用しようとする旨の指示を入力する。

【0018】すると、CPU22がカードスロット21に挿入されているカードメモリ1からユーザ名と認証コードとを読み出す。ここでは、説明のために、ユーザ名は「TKAYA」であり、対応する認証コードは「TK1」とであるとする。

【0019】そして、CPU22が取扱者管理メモリ23からユーザ名「TKAYA」を検索し、それに対応して取扱者管理メモリ23に格納されているパスワード「1」を読み出す。

【0020】そして、CPU22が表示部24にパスワードの入力を要求するメッセージを表示出力する。ここで、利用者がCPU22にパスワード「1」を入力すると、CPU22が取扱者管理メモリ23に格納されているパスワード「1」と入力されたパスワード「1」とが一致するので、さらに、取扱者管理メモリ23からユーザ名「TKAYA」に対応する認証コード「TK1」を読み出す。

【0021】そして、読み出した認証コード「TK1」と、カードメモリ1に格納されている認証コード「TK1」と一致するかを調べると、それらが一致しているので、装置の使用を許可する。そして、利用者は、装置を操作できるようになる。

【0022】次に、図2に示す認証システムの各部を具

体的に説明する。ここで、カードスロット21と、表示部24と、操作部25とは、図1に示すものと同様のものであるので、説明を省略する。また、サーバ3における取扱者管理メモリ33は、図1に示す取扱者管理メモリ23と同様のものであるので、説明を省略する。

【0023】CPU22は、図1に示すCPU22と同様のものであるが、図6に示す処理S4に代わって、サーバ3に送受信部26を介してカードメモリ1から読み出したユーザ名に対応するパスワードを要求し、当該パスワードを受信するようになっていところと、処理S8に代わって、サーバ3に送受信部26を介してカードメモリ1から読み出したユーザ名に対応する認証コードを要求し、当該認証コードを受信するようになっていところとが異なっている。

【0024】サーバ3のCPU32は、送受信部31を介して認証装置のCPU22からパスワードの要求を受けて、取扱者管理メモリ33からパスワードを検索して送信出力するものであり、また、送受信部31を介して認証装置のCPU22から認証コードの要求を受けて、取扱者管理メモリ33から認証コードを検索して送信出力するものである。

【0025】従って、図2に示す認証装置は、取扱者管理メモリ23を検索する代わりに、当該検索の指示をサーバ3に送信出力する以外は、図1に示す認証装置と同様の動作をするものである。

【0026】

【発明が解決しようとする課題】しかしながら、上記認証装置及び認証システムにおける従来の認証方法では、カードメモリがパスワードを知り得る者によって不正にコピーされると、装置が不正使用される虞があり、また、そのような不正使用により装置を操作した記録が残らないという問題点があった。

【0027】本発明は上記実情に鑑みて為されたもので、より高度に不正使用を防止し、不正使用の記録を残すことができる認証装置及び認証システムを提供することを目的とする。

【0028】

【課題を解決するための手段】上記従来例の問題点を解決するための請求項1記載の発明は、認証装置において、認証が為される毎に認証コードを変更することの特徴としており、以前使用した認証コードを用いては認証を行えず、不正使用を防止できる。

【0029】上記従来例の問題点を解決するための請求項2記載の発明は、認証装置において、メモリカードのインターフェイスであるカードスロットと、認証コードを格納する取扱者管理メモリとを具備し、認証が為されると、前記取扱者管理メモリに格納されている認証コードを特定のコードで上書きして変更し、前記カードスロットに挿入されたメモリカードの認証コードを前記特定のコードで上書きして変更することの特徴としており、

メモリカードから認証コードを不正にコピーした場合に、その後一度でも正規のメモリカードを用いて認証を行っていただければ、不正にコピーした認証コードでは認証を行えず、不正使用を防止できる。

【0030】上記従来例の問題点を解決するための請求項3記載の発明は、認証システムにおいて、メモリカードのインターフェイスであるカードスロットを具備する認証装置と、認証コードを格納する取扱者管理メモリを具備するサーバとを備え、前記認証装置で認証が為されると、前記認証装置が特定のコードとともに前記サーバに前記取扱者管理メモリに格納されている認証が為された認証コードを当該特定のコードで上書きして変更する要求を送信出力し、前記カードスロットに挿入されたメモリカードの認証コードを前記特定のコードで上書きして変更し、前記サーバが、受信した前記要求にしたがって、前記取扱者管理メモリに格納されている前記認証コードを前記特定のコードで上書きして変更することの特徴としており、メモリカードから認証コードを不正にコピーした場合に、その後一度でも正規のメモリカードを用いて認証を行っていただければ、不正にコピーした認証コードでは認証を行えず、不正使用を防止できる。

【0031】上記従来例の問題点を解決するための請求項4記載の発明は、請求項2記載の認証装置において、認証が為されないと、当該認証が為されなかったユーザ名による装置の使用を以後できないようにすることの特徴としており、請求項2記載の効果に加えて、不正な利用者の継続的な装置の不正使用を防止できる。

【0032】上記従来例の問題点を解決するための請求項5記載の発明は、請求項3記載の認証システムにおいて、認証が為されないと、当該認証が為されなかったユーザ名による装置の使用を以後できないようにすることの特徴としており、請求項3記載の効果に加えて、不正な利用者の継続的な装置の不正使用を防止できる。

【0033】上記従来例の問題点を解決するための請求項6記載の発明は、請求項2又は請求項4記載の認証装置において、特定のコードは、認証が為された時刻を表すコードであることを特徴としており、請求項2又は請求項4記載の効果に加えて、不正使用が何時頃為されたのかを知ることができる。

【0034】上記従来例の問題点を解決するための請求項7記載の発明は、請求項3又は請求項5記載の認証装置において、特定のコードは、認証が為された時刻を表すコードであることを特徴としており、請求項3又は請求項5記載の効果に加えて、不正使用が何時頃為されたのかを知ることができる。

【0035】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら説明する。本発明の実施の形態に係る認証装置（本装置）及び認証システムは、装置の使用を許可する毎に認証コードを変更するもので、不正使用を防

止するとともに、不正使用が為された場合には、その事実を後に知ることができるものである。

【0036】本装置は、図1に示した一般的な認証装置と同様の構成を備えるものであるが、CPU22における処理が少々異なっている。そこで以下、CPU22における処理について説明する。

【0037】本装置のCPU22は、従来と同様に、図6に示す処理を行うものであるが、処理S9において、処理S3にてカードメモリ1から読み出した認証コードと取扱者管理メモリ23から読み出した認証コードとが一致して（Yesであり）、認証が達成され、装置の操作を許可する処理S10を処理する直前に、特定の 방법으로認証コードを新たに生成し、取扱者管理メモリ23とカードメモリ1とに当該新たに生成した認証コードを書き込む処理（以下、「認証コード更新処理」と称する）を行うものである。

【0038】ここで、CPU22の認証コード更新処理について、図3を用いて具体的に説明する。図3は、本装置におけるCPU22の認証コード更新処理を表すフローチャート図である。まず、CPU22は、認証コード更新処理を行うに当たって、メモリカード1がカードスロット21に挿入されているか否かを調べる（S21）。そして、メモリカード1がカードスロット21に挿入されていないならば（Noならば）、表示部24にメモリカードの挿入を要求するメッセージを表示出力し（S22）、処理S21に移行する。

【0039】また、処理S21において、メモリカード1がカードスロット21に挿入されていれば（Yesならば）、新たに認証コードを生成し（S23）、当該新たに生成した認証コードをカードメモリ1の認証コードに上書きして格納する（S24）。

【0040】そして、CPU22は、処理S23で生成した認証コードを、メモリカード1に格納されているユーザ名に対応して取扱者管理メモリ23に格納されている認証コードに上書きして格納し（S25）、処理終了する。

【0041】尚、処理S23において認証コードを生成する方法として、例えば時刻を用いる方法が考えられる。すなわち、CPU22が処理S23を実行する時刻が15時23分19秒であったとすれば、認証コードとして「152319」を用いることとすればよい。このようにすれば、前回不正使用があった時刻を取扱者管理メモリ23の内容として記録することができる効果がある。

【0042】次に本装置の動作について説明する。尚、正規のメモリカード1の内容をコピーした不正なメモリカード1'が不正な利用者によって生成されているとする。ここで、正規のメモリカード1と不正なメモリカード1'とは同様のメモリカードであるが、区別のために符号を違えている。

【0043】正規の利用者が正規のメモリカード1を本装置に挿入し、従来と同様にパスワードを入力すると、前回装置を使用した際に書き込まれている認証コード、例えば「120000」が取扱者管理メモリ23とメモリカード1とに格納されており、それらが一致するので、装置が操作できるようになる。

【0044】また、このとき、新たに認証コードが生成され、当該認証コード、例えば「152319」が取扱者管理メモリ23とメモリカード1とに格納される。やがて、不正利用者が不正なメモリカード1'を本装置に挿入し、パスワードを入力するが、当該不正なメモリカード1'には、メモリカード1を不正にコピーした際の認証コード、例えば「120000」が格納されており、取扱者管理メモリ23には変更された認証コードである「152319」が格納されているため、両者が一致せず、不正な利用者は、装置を操作することができない。

【0045】本装置によれば、メモリカードが不正にコピーされても、コピーされてから一度でも正規のメモリカードを認証装置に挿入し、装置を操作すれば、取扱者管理メモリと当該正規のメモリカードとに格納されている認証コードが変更されるので、不正にコピーされたメモリカードを用いて装置を操作することができなくなり、不正使用を防止できる効果がある。

【0046】また、本装置によれば、不正にコピーされたメモリカードを利用して装置が操作されると、当該不正にコピーされたメモリカードと取扱者管理メモリとに格納されている認証コードが変更されるので、次に正規のメモリカードを挿入しても装置を使用することができなくなるため、不正使用があったことを知ることができ、不正使用を記録できる効果がある。

【0047】本発明の実施の形態に係る認証システム（本システム）は、図2に示す認証システムと同様に、CPU22が図6の処理S4とS8との代わりに、サーバ3に対して特定のユーザ名に対するパスワードと認証コードとを要求して受信するようになっており、また、図3の処理S25の代わりに、サーバ3に対して特定のユーザ名に対する認証コードを書き換える要求を送信出力するものである。

【0048】この場合のサーバ3のCPU32は、特定のユーザ名に対する認証コードを書き換える要求をユーザ名と、新たな認証コードとともに送受信部31を介して受信して、当該新たな認証コードを当該ユーザ名に対応して取扱者管理メモリ33に格納されている認証コードに上書きして格納するようにすればよい。

【0049】さらに、本装置及び本システムは、利用者がメモリカード1を用いて認証を行ったが、本装置の取扱者管理メモリ23又は本システムのサーバ3の取扱者管理メモリ33に格納されている認証コードと、当該メモリカード1に格納されている認証コードとが一致せ

ず、認証が為されないと、当該ユーザ名による装置の使用を今後停止するものであっても構わない。

【0050】つまり、CPU22が図6に示す処理S9において、認証コードが一致しないと（Noである）、処理S11によりカードメモリ1が異なる旨のメッセージを表示出力するとともに、当該ユーザ名による装置の使用を今後停止する。

【0051】当該ユーザ名による装置の使用を停止するためには、例えば、図3に示した処理S23と同様に認証コードを生成して、処理S25と同様に本装置の取扱者管理メモリ23又は本システムのサーバ3の取扱者管理メモリ33における当該ユーザ名に対応する認証コードのみを新しく生成された認証コードで上書きし、カードメモリ1には上書きしないようにすることが考えられる。

【0052】このようにした本装置又は本システムによれば、メモリカード1から認証コードを不正にコピーした場合に、正規の利用者よりも先に、当該不正なメモリカード1を所持する不正な利用者が一度でも使えば、取扱者管理メモリにおける認証コードが変わり、次に正規のカードメモリ1を用いて正規の利用者が認証を行おうとすると、認証コードが異なるため、当該ユーザ名による装置の使用ができなくなり、正規の利用者も装置の使用ができなくなるが、不正な利用者の継続的な装置の不正使用を防止できる効果がある。

【0053】

【発明の効果】請求項1記載の発明によれば、認証が為される毎に認証コードを変更する認証装置としているので、以前使用した認証コードを用いては認証を行えず、不正使用を防止できる効果がある。

【0054】請求項2記載の発明によれば、認証が為されると、取扱管理者メモリの認証コードとカードスロットに挿入したメモリカードの認証コードを同じ認証コードに変更する認証装置としているので、メモリカードから認証コードを不正にコピーした場合に、その後一度でも正規のメモリカードを用いて認証を行っていれば、不正にコピーした認証コードでは認証を行えず、不正使用を防止できる効果がある。

【0055】請求項3記載の発明によれば、認証が為されると、サーバ上の取扱管理者メモリの認証コードとカードスロットに挿入したメモリカードの認証コードを同じ認証コードに変更する認証システムとしているので、メモリカードから認証コードを不正にコピーした場合に、その後一度でも正規のメモリカードを用いて認証を行っていれば、不正にコピーした認証コードでは認証を行えず、不正使用を防止できる効果がある。

【0056】請求項4記載の発明によれば、認証が為されないと、当該認証が為されなかったユーザ名による装置の使用を以後できないようにする請求項2記載の認証装置としているので、メモリカードから認証コードを不

正にコピーした場合に、正規の利用者よりも先に、不正な利用者が一度でも不正なカードを用いて装置を使用すれば、取扱者管理メモリにおける認証コードが変わることとなり、その後正規のカードメモリを用いて正規の利用者が認証を行おうとすると、認証コードが異なるため、当該ユーザ名による装置の使用を停止して、不正な利用者の継続的な装置の不正使用を防止できる効果がある。

【0057】請求項5記載の発明によれば、認証が為されないと、当該認証が為されなかったユーザ名による装置の使用を以後できないようにする請求項3記載の認証システムとしているので、メモリカードから認証コードを不正にコピーした場合に、正規の利用者よりも先に、不正な利用者が一度でも不正なカードを用いて装置を使用すれば、取扱者管理メモリにおける認証コードが変わることとなり、その後正規のカードメモリを用いて正規の利用者が認証を行おうとすると、認証コードが異なるため、当該ユーザ名による装置の使用を停止して、不正な利用者の継続的な装置の不正使用を防止できる効果がある。

【0058】請求項6記載の発明によれば、特定コードを認証が為された時刻を表すコードとした請求項2又は請求項4記載の認証装置としているので、請求項2又は請求項4記載の効果に加えて、不正使用が何時頃為され

たのかを知ることができる効果がある。

【0059】請求項7記載の発明によれば、特定コードを認証が為された時刻を表すコードとした請求項3又は請求項5記載の認証装置としているので、請求項3又は請求項5記載の効果に加えて、不正使用が何時頃為されたのかを知ることができる効果がある。

【図面の簡単な説明】

【図1】認証装置の構成ブロック図である。

【図2】認証システムの構成ブロック図である。

【図3】本装置におけるCPU22の認証コード更新処理を表すフローチャート図である。

【図4】カードメモリ1に格納されているテーブルの内容の一例を表す説明図である。

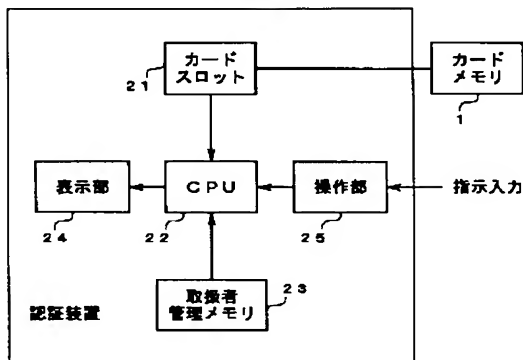
【図5】取扱者管理メモリ23の内容の一例を表す説明図である。

【図6】CPU22における認証の処理を表すフローチャート図である。

【符号の説明】

1…カードメモリ、 21…カードスロット、 22…CPU、 23…取扱者管理メモリ、 24…表示部、 25…操作部、 26…送受信部、 3…サーバ、 31…送受信部、 32…CPU、 33…取扱者管理メモリ

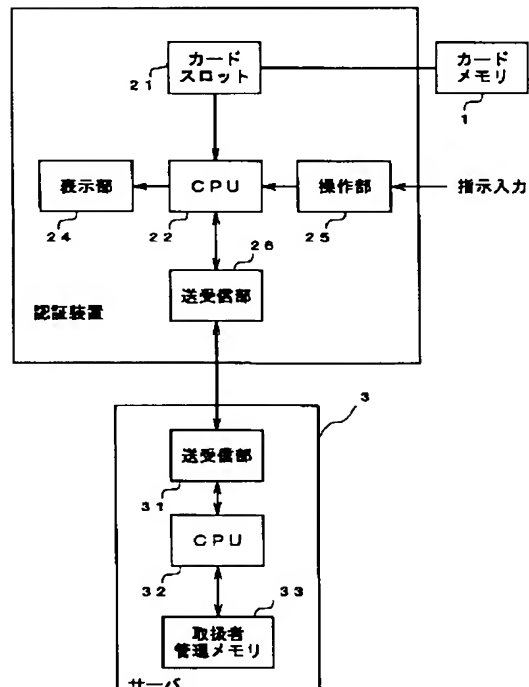
【図1】



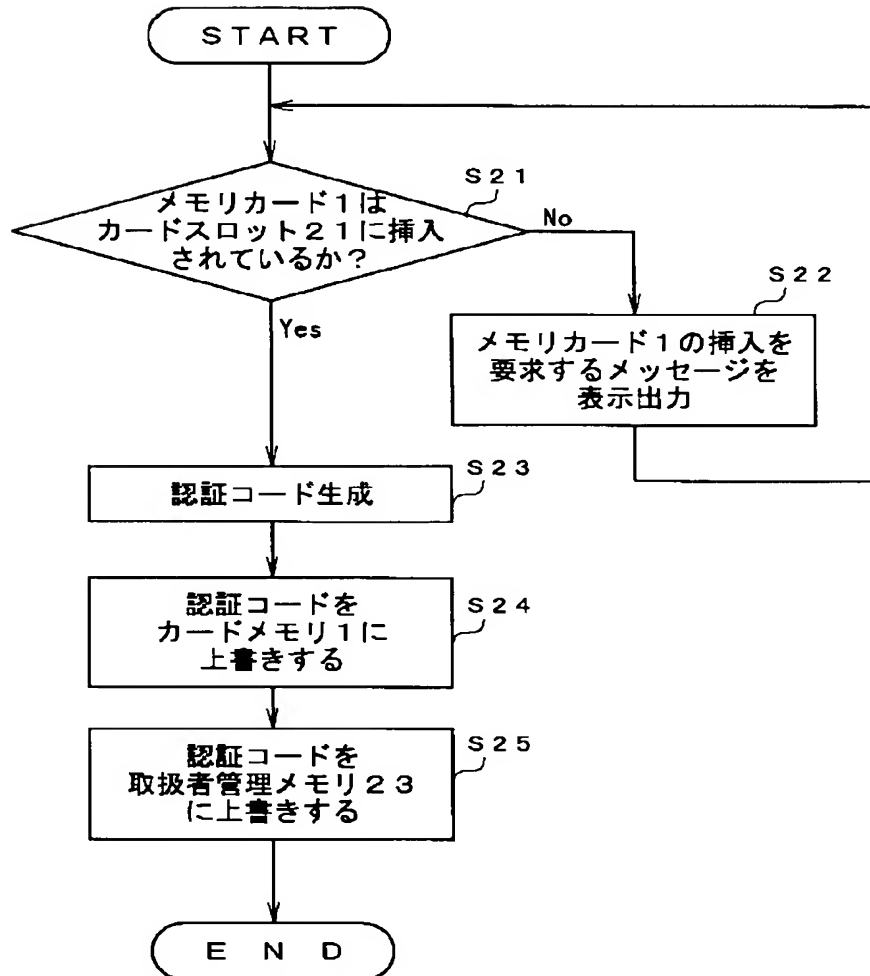
【図4】

ユーザー名	認証コード
TKAYA	TK1

【図2】



【図 3】



【図 5】

ユーザー名	パスワード	認証コード
TKAYA	1	TK1
ABC	XYZ	AABBCC
ICHIRO	16	7
⋮	⋮	⋮
⋮	⋮	⋮
⋮	⋮	⋮



【図6】

